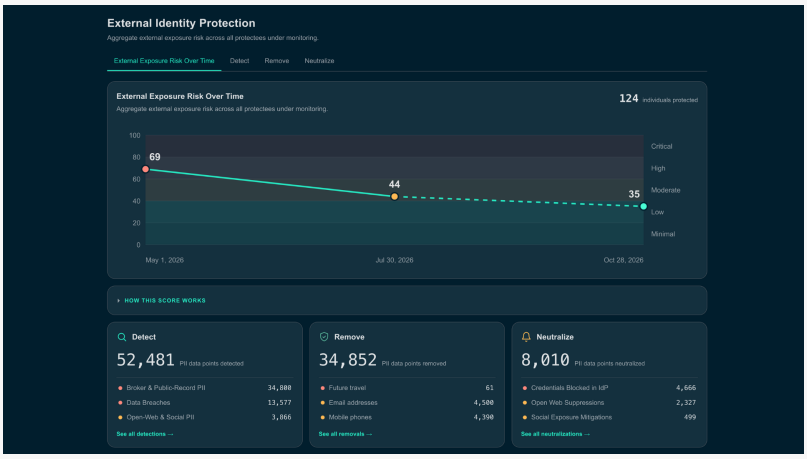
VanishID Launches External Identity Protection at Black Hat 2026, the First Security Control for Exposed Identity Data

Attackers target access, not titles. External Identity Protection secures the exposed identity data used to target executives, families, and key employees.



VanishID's External Identity Protection dashboard tracks exposure risk across all monitored individuals. The platform shows exposed identity data detected, removed, and neutralized.

LAS VEGAS, NV, UNITED STATES, August 3, 2026 /EINPresswire.com/ -- VanishID, the external identity security company, today launched External Identity Protection, a continuous security control for the exposed personal data attackers use against high-value personnel. The control covers executives and boards, the employees whose access makes them targets, and their families. It finds their exposure wherever it lives, wipes out what it can, and neutralizes residual risk. VanishID will demonstrate it publicly for the first time this week at Black Hat USA 2026.

> External Identity Protection takes the attacker's raw material away continuously, and it protects the people attackers actually target."
>
> *Matt Polak, CEO of VanishID*

External Identity Protection in Brief

- VanishID launched External Identity Protection, the first continuous security control for the exposed personal data attackers use against executives, high-access employees like assistants and help desk staff, and their families.

- AI has industrialized attacks on people. Generative AI made convincing, personal attacks cheap and instant. Verizon's 2026 Data Breach Investigations Report finds 65% of AI-assisted attacks target people, and every one of them runs on the same fuel: the exposed personal data of targets.

- External Identity Protection uses four types of AI agents to detect, analyze, remove, and

neutralize personal data exposure across data brokers, people-search sites, social media, breach and credential dumps, the dark web, and public records, addressing a gap that identity management, endpoint protection, and awareness training don't cover.

VanishID customers typically see an 85% reduction in attacker-reachable personal data within 90 days, including a 93% drop in data broker profiles. Onboarding requires only a name and corporate email, with no employee effort or added security headcount.

External Identity Protection complements identity management, identity threat detection and response, endpoint security, email security, and security awareness training by informing and contextualizing publicly exposed identity risks those internal technologies cannot see.

“Every other tool defends what a company owns. We defend the one thing a company can’t patch, the public personal data of its people,” said Matt Polak, CEO of VanishID. “External Identity Protection takes the attacker’s raw material away continuously, and it protects the people attackers actually target. That list reaches far beyond the C-Suite. It’s anyone whose access makes them worth attacking, or whose authority makes them worth impersonating.”

Why Existing Security Controls Leave a Gap

The same people are protected inside the perimeter and exposed outside it. Inside, identity management, endpoint protection, and awareness training cover them. Outside, threat intelligence feeds reports on threat actor tactics, techniques, and procedures (TTPs), as well as lagging indicators of compromise (IOCs), neither of which tells a security team which employees are most likely to be targeted, why, and how. Today, nothing in the security stack measures external identity exposure at population scale, let alone reduces it. VanishID’s innovations solve this problem for the first time.

VanishID’s agents have removed more than 10 million exposed records for customers. VanishID’s research across 10,000 US executives found nearly everyone already exposed, cleartext passwords sitting on the dark web, breach histories dozens deep, a home address one search away. An attacker can plan an entire campaign from that data without touching company infrastructure, so nothing fires an alert and the SOC never sees it coming. That is the gap VanishID was built for. MITRE ATT&CK calls this reconnaissance, Gather Victim Identity Information (T1589), a technique that “cannot be easily mitigated with preventive controls,” where the only defense is reducing the data available to attackers.

“It's long overdue for converged security (cyber-physical) to apply to humans through identity

security. Agentic deployment enables next-level identity security and threat actors will be disappointed as a result," said Jim Routh, six-time former CISO.

Why Attackers Target People Instead of Systems

Because attackers target access, the highest-value target is often not the executive. It is the executive assistant who executes the CFO's instructions, the help desk lead who resets credentials, or the finance manager who approves payments. Internal tools see these employees as low risk because they focus on internal telemetry: MFA is on and the device is patched. Attackers see them as ideal targets because they are fully exposed and easy to impersonate, and they hold privileged access. These attacks are succeeding right now. Verizon's 2026 Data Breach Investigations Report ties 35% of breaches to attacks that start with people, through phishing, credential abuse, and pretexting. That is ahead of the 31% that start with vulnerability exploits, where most security budgets still go. In April, attackers socially engineered a single Carnival employee and exposed the personal data of nearly 6 million people.

Why AI Changes the Economics of Attacks

AI is widening the gap because generative AI mass-produces the attack. AI attacks aim, deliver, and convince using the same fuel: the exposed personal data of targets. Generative AI made a convincing, personal attack cheap and instant. Verizon's 2026 Data Breach Investigations Report finds 65% of AI-assisted attacks target people, nearly double the all-breach rate. Defenders can't out-detect every fake, but they can drain the fuel and neutralize residual risk. Because these attacks share one source, mitigating it disrupts all of them at once, at reconnaissance, the earliest and cheapest place to break the chain.

Why Continuous Protection Matters

Until now, organizations attacked fragments of the problem. Manual removals, often underpinned by consumer data broker removal services, filed opt-outs one site at a time and lost ground to sources that repopulate within weeks. Dark web monitoring flagged stolen credentials but left the fixing to someone else. Awareness training coached people to spot the lure instead of removing what made the lure convincing. Breach dumps and public records persist no matter who files the paperwork, and that residual risk sits unmitigated and invisible to the SOC. Nothing was continuous, and nothing covered the whole surface, while AI weaponized new exposure within hours. Only agents keep pace with agents.

How External Identity Protection Works

External Identity Protection runs four classes of purpose-built agents, continuously and at machine speed.

1. Detection agents never stop searching. They scan data brokers and people-search sites, social

platforms, breach and credential dumps, the dark web, and public records for exposed identity data. When a source only renders in a browser, they drive real browsers with combined vision and page understanding, reaching pages that block conventional crawlers.

2. Analyst agents think like an attacker. They investigate a person the way an adversary would, correlating exposure into a single picture, then scoring who is at risk, why, and how urgently, before an incident.

3. Remediation agents remove what can be neutralized. They execute takedowns across brokers, people-search sites, and exposed social footprints, work each site's opt-out steps, verify every result, and repeat as data returns.

4. Residual-risk agents watch what cannot be removed. Where exposure persists, in breach dumps and public records, they suppress and neutralize risk, and alert the SOC to what remains and to re-exposure over time.

The platform never trains on personal data and is SOC 2 Type II certified. Guardrails are architectural, with domain allow-lists, hard step ceilings, and full decision trails, and edge cases route to a human analyst. PII stays out of logs and telemetry.

Proven Results

The results are measurable. Within 90 days, customers typically see an 85% drop in the PII an attacker can reach, including a 93% reduction in data broker profiles, and the platform holds the surface down as new exposure appears. Deployment is turnkey. Onboarding takes a name and a corporate email, and the platform runs with no lift for employees and no new headcount for security.

Black Hat USA 2026 attendees can see External Identity Protection live, including the new External Identity Dashboard, at the VanishID Booth #5813, August 4–6, and can request a free exposure assessment on one executive to see exactly what an attacker sees today.

External Identity Protection is available now. Rollout to VanishID's existing customer base will continue throughout the year. To schedule a demo at Black Hat or learn more, visit vanishid.com/black-hat.

About VanishID

VanishID is the external identity security company. Its agentic AI platform puts autonomous agents to work finding and neutralizing the exposed personal information attackers use against executives, employees, and their families. The agents hunt exposure the way an adversary would, at machine speed, across data brokers, breach dumps, the dark web, and public records. They remove what they can and mitigate residual risk. Onboarding takes a name and a corporate

email, with no lift for the security team. The platform never trains on personal data and is SOC 2 Type II certified. More than 100 organizations rely on VanishID, from Fortune 500 enterprises and financial institutions to health systems and public sector agencies. Founded in 2019 and headquartered in Bethesda, Maryland, VanishID is backed by Dell Technologies Capital, Crosslink Capital, Rally Ventures, Energy Impact Partners, Bright Pixel, LockStep Ventures, and strategic angels including former Palo Alto Networks CEO Mark McLaughlin and former Mandiant CPO Christopher Key.

Learn more at vanishid.com.

Marketing at VanishID
VanishID
email us here
Visit us on social media:
LinkedIn
YouTube
X
